RECORD AND BRIEFS

No. 16-402

FILED
AUG 14 2017
OFFICE OF THE CLERK
SUPREME COURT, U.S.

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

—v.—

UNITED STATES OF AMERICA,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

BRIEF OF SCHOLARS OF CRIMINAL PROCEDURE AND PRIVACY AS *AMICI CURIAE* IN SUPPORT OF PETITIONER

ANDREW G. FERGUSON
UDC DAVID A. CLARKE SCHOOL OF LAW
4340 Connecticut Avenue
Washington, D.C. 20008

HARRY SANDICK
Counsel of Record
KATHRINA SZYMBORSKI
JARED BUSZIN
PATTERSON BELKNAP WEBB & TYLER LLP
1133 Avenue of the Americas
New York, New York 10036
(212) 336-2000
hsandick@pbwt.com

Counsel for Amici Curiae

August 14, 2017

TABLE OF CONTENTS

Page

INTEREST OF *AMICI CURIAE* 1

SUMMARY OF ARGUMENT 2

ARGUMENT 3

I. EXTENSION OF *SMITH*'S REASONING WOULD POTENTIALLY EVISCERATE CITIZENS' PRIVACY IN THE DIGITAL AGE 3

A. Society's Relationship with Technology Has Changed Both Quantitatively and Qualitatively Since *Smith* 4

B. *Smith* Addressed a Radically Different Context Than This Case and Should Be Limited to Its Facts 8

II. THE THIRD-PARTY DOCTRINE HAS BEEN WIDELY CRITICIZED BY SCHOLARS 14

A. The Third-Party Doctrine Is Based on a Questionable Theory of Privacy 16

B. The Third-Party Doctrine Does Not Match Expectations of Privacy in the Digital Age 19

C. Justifications for the Third-Party Doctrine Do Not Hold Up in the Digital Age 21

CONCLUSION 27

TABLE OF AUTHORITIES

Page(s)

CASES

United States v. Benford,
2010 WL 1266507 (N.D. Ind. March 26, 2010) 10

Chapman v. United States,
365 U.S. 610 (1961) 23

Commonwealth v. Estabrook,
472 Mass. 852 (2015) 8

State v. Earls,
70 A.3d 630 (N.J. 2013) 9

Ferguson v. City of Charleston,
532 U.S. 67 (2001) 16

Georgia v. Randolph,
547 U.S. 103 (2006) 22

Hoffa v. United States,
385 U.S. 293 (1966) 17

United States v. Jeffers,
342 U.S. 48 (1951) 23

United States v. Jones,
565 U.S. 400 (2012) 6, 20

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

In re Application of the United States for an Order Authorizing the Installation & Use of a Pen Register & a Caller Identification System on Telephone Numbers, 402 F. Supp. 2d 597 (D. Md. 2005) 10

In re Application of the United States for Historical Cell Site Data, 2010 WL 4286365 (S.D. Tex. Oct. 29, 2010) 10

Katz v. United States, 389 U.S. 347 (1967) 3, 17, 18

Kyllo v. United States, 533 U.S. 27 (2001) 12

United States v. Maynard, 615 F. 3d 544 (D.C. Cir. 2010) 12

Packingham v. North Carolina, 137 S. Ct. 1730 (2017) 6

People v. Weaver, 12 N.Y.3d 433 (2009) 12, 13

Riley v. California, 134 S. Ct. 2473 (2014) 6, 7, 23, 24

Smith v. Maryland, 442 U.S. 735 (1979) ..... passim

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

Stoner v. California,
376 U.S. 483 (1964) 23

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 20

STATUTES

18 U.S.C. § 2511(2)(a) 18

OTHER AUTHORITIES

Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 Vand. L. Rev. 1289 (1981) 15, 16

Jack M. Balkin, *Essay: The Constitution in the National Surveillance State*, 93 Minn. L. Rev. 1 (2008) 18

James Beck et al., *The Use of Global Positioning (GPS) and Cell Tower Evidence to Establish a Person's Location—Part II*, 49 Crim. Law. Bull. 8 (Summer 2013) 9

Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law*, 30 Harv. J.L. & Tech. 1 (2016) 20

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 Fordham L. Rev. 611 (2014) 17

Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & Pol'y 211 (2006) 18, 23

Nate Cardozo et al., *Who Has Your Back?: Protecting Your Data from Government Requests*, Elec. Frontier Found. (July 2017) 25

Brian Clark, *The Company Behind Roomba Cleaner Wants to Sell Home Data to Apple, Amazon, or Google*, Business Insider (July 25, 2017) 7

Sherry Colb, *What Is a Search: Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 Stan. L. Rev. 119 (2002) 18

Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 Calif. L. Rev. 1593 (1987) 23

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

Chris Conley, *Non-Content Is Not Non-Sensitive: Moving Beyond the Content/non-Content Distinction*, 54 Santa Clara L. Rev. 821 (2014) 19

CTIA, *Annual Year-End 2016 Top-Line Survey Results*, https://www.ctia.org/docs/default-source/default-document-library/annual-year-end-2016-top-line-survey-results-final.pdf?sfvrsn=2 12

Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 Berkeley Tech. L.J. 1199 (2009) 21

Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. Pa. L. Rev. 327 (2015) 6

Andrew Guthrie Ferguson, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT (2017) 22

Andrew Guthrie Ferguson, *The Smart Fourth Amendment*, 102 Cornell L. Rev. 547 (2017) 5

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681 (2011) 10

Susan Freiwald, *First Principles of Communications Privacy*, 2007 Stan. Tech. L. Rev. 3 (2007) 18

Government Accountability Office, Center for Science, Technology and Engineering, *Technology Assessment: Internet of Things, Status and Implication of an Increasingly Connected World*, GAO-17-75 (May 2017) 5

Government Requests Report, Facebook, https://govtrequests.facebook.com/country/United%20States/2016-H2/ 26

Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 Pepp. L. Rev. 975 (2007) 20

Stephen E. Henderson, *Carpenter v. United States and the Fourth Amendment: The Best Way Forward*, 26 William & Mary Bill of Rights J. (forthcoming 2017) 12

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 Cath. U. L. Rev. 373 (2006) 9

Stephen Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 Iowa L. Rev. Bull. 39 (2011) 18

Spenser Hsu, *Court: Warrantless Requests to Track Cellphones, Internet Use Grew Sevenfold in D.C. in Three Years*, Wash. Post (July 18, 2017)..... 13

Internet/Broadband Fact Sheet, Pew Research Center (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/internet-broadband/..... 4

Margot E. Kaminski, *Robots in the Home: What Will We Have Agreed To?*, 51 Idaho L. Rev. 661 (2015)..... 7

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. Rich. L. Rev 465 (2015) 14

Orin S. Kerr, *Applying the Fourth Amendment to Internet Communications: A General Approach*, 62 Stan. L. Rev. 1005 (2010) 25

Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561 (2009) 15, 21, 20

Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 Sup. Ct. Rev. 205 (2015)..... 15

Wayne R. La Fave, SEARCH AND SEIZURE, A TREATISE ON THE FOURTH AMENDMENT (5th ed. 2012) 16

Law Enforcement Requests, Lyft, https://help.lyft.com/hc/en-us/articles/214218437-Law-Enforcement-Requests 25

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 Mich. L. Rev. 1229 (1983) 19

Lyft Information Request Report – 2015, Lyft, https://lyft-assets.s3.amazonaws.com/helpcenter/Drive%20With%20Lyft/Lyft%20Transparency%20Report%20-%202015%20(1).pdf 26

Alex Matthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior* (April 29, 2015) 14

Jonathan Mayer, Patrick Mutchler, & John C. Mitchell, *Evaluating the Privacy Properties of Telephone Metadata*, 113 PNAS 5536 (May 17, 2016) 7

Mobile Fact Sheet, Pew Research Center (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/ 4

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557 (2004) 18

OECD Digital Economy Outlook (Paris: OECD Publishing, 2015), http://dx.doi.org/10.1787/9789264232440-en 5

Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 Tex. L. Rev. 85 (2014) 5

Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934 (2013) 13

Jed Rubenfeld, *The End of Privacy*, 61 Stan. L. Rev. 101 (2008) 18

Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, 2011 U. Ill. J.L. Tech. & Pol'y 281 (2011) 22

Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 Cardozo L. Rev. 643 (2013) 20

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

Christopher Slobogin, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007) 15, 18, 22

Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. Law Rev. 1083 (2002) 15, 18

Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 Md. L. Rev. 614 (2011) 20

Scott E. Sundby, *Everyman's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 Colum. L. Rev. 1751 (1994) 19

Matthew Tokson, *Automation and the Fourth Amendment*, 96 Iowa L. Rev. 581 (2011) 5, 17, 23, 24

Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 Nw. U. L. Rev. 139 (2016) 11, 15

Transparency Report, Uber, https://transparencyreport.uber.com/ 26

TABLE OF AUTHORITIES (CONTINUED)

Page(s)

James Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward An Expanded Vision of the Fourth Amendment Privacy Province*, 36 Hastings L.J. 645 (1985) 19

U.S. Department of Commerce Internet Policy Taskforce & Digital Economy Leadership Team, *Fostering the Advancement of the Internet of Things* (Jan. 2017) 4

Uber Guidelines for Law Enforcement Authorities, Uber, https://www.uber.com/legal/data-requests/guidelines-for-law-enforcement-united-states/en-US/ 25

Cleve R. Wootson, Jr., *A Man Detailed His Escape from a Burning House. His Pacemaker Told Police a Different Story*, Wash. Post (Feb. 8, 2017) 24

INTEREST OF *AMICI CURIAE*[1]

Amici curiae are forty-two scholars engaged in significant research and/or teaching on criminal procedure and privacy law. *See* Appendix A (listing individual scholars joining this brief). This brief addresses issues that are within *amici*'s particular areas of scholarly expertise. They have a shared interest in clarifying the law of privacy in the digital era, and believe that a review of scholarly literature on the topic is helpful to answering the question in this case.

---

[1] Pursuant to Rule 37.6, *amici curiae* certifies that this brief was not written in whole or in part by counsel for any party, and no person or entity other than *amici curiae* and its counsel has made a monetary contribution to the preparation and submission of this brief. Letters from the parties consenting to the filing of this brief have been filed with the Clerk of the Court.

SUMMARY OF ARGUMENT

This case presents an opportunity to reconsider the Fourth Amendment in the digital age. Cell phones are only one of the many new and pervasive digital technologies which automatically collect and reveal intimate personal data, such as Cell Site Location Information ("CSLI"), to third parties. This Court should resist extending the reasoning of *Smith v. Maryland*, 442 U.S. 735 (1979) -a 38-year-old case built on a faulty privacy premise—to the modern, hyper-connected, technology-dependent world. Instead, the Court should recognize that the new realities of this world require new legal doctrines to fit the privacy expectations shared by most Americans.

Criminal procedure and privacy scholars are in near-unanimous agreement that an extension of what some have called the "third-party doctrine," which holds that people lack a reasonable expectation of privacy in information voluntarily conveyed to third parties, could eliminate citizens' privacy in the modern age. CSLI (and other data transmitted to third parties in the modern age) can reveal an individual's interests, friendships, activities, travel, associations, beliefs, health concerns, financial problems, employment, and education. *Smith* is grounded in a pre-digital era, and cannot support future application of the Fourth Amendment.

The trajectory and pace of technological change further counsels against extending *Smith*. As the use of "smart" devices and their related applications steadily grows among Americans, so too does the volume, scope, detail, and type of intimate data

transmitted to third parties. An extension of *Smith*'s reasoning would give law enforcement ever-increasing access to the most private details of individuals' lives without a warrant or probable cause.

As a matter of Fourth Amendment practice, extending the third-party doctrine would curtail digital privacy and encourage arbitrary government intrusions into the lives of American citizens. As a matter of Fourth Amendment theory, applying the third-party doctrine to the digital world would undersell the value of privacy, and contradict the logic of *Katz v. United States*, 389 U.S. 347, 359 (1967) (1967) ("Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."). And, as a matter of precedent, *Smith* offers an inapposite and inadequate doctrinal foundation to support the future of a digital Fourth Amendment.

ARGUMENT

I. EXTENSION OF *SMITH*'S REASONING WOULD POTENTIALLY EVISCERATE CITIZENS' PRIVACY IN THE DIGITAL AGE

The Government and the Sixth Circuit both relied heavily on *Smith v. Maryland* in this case, drawing an analogy between the dialed phone numbers addressed in *Smith* and the CSLI addressed here. But the analogy is flawed on both technological and doctrinal grounds. Given the profound technological advances of the last 38 years—and

society's drastically changed relationship with technologies requiring third-party providers—upholding CSLI tracking on the basis of parallels to long-obsolete technology would lead to a substantial reduction in privacy in the modern era. This Court should limit the holding of *Smith* to its particular facts.

A. Society's Relationship with Technology Has Changed Both Quantitatively and Qualitatively Since Smith

The embrace of digital third-party services has quantitatively and qualitatively reshaped society's relationship with technology. The vast majority of Americans today are digital citizens—and reliance on connected devices is only growing. Pew Research Center reports that today 95 percent of adult Americans use cell phones, 90 percent use the Internet, 77 percent own smartphones, and 70 percent use social media.[2] The U.S. Department of Commerce Internet Policy Taskforce estimates that "between the years of 2015 and 2020, the number of connected devices in the United States will nearly double from 2.3 billion to 4.1 billion."[3] The

---

[2] *Mobile Fact Sheet*, Pew Research Ctr. (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/mobile/; *Internet/Broadband Fact Sheet*, Pew Research Ctr. (Jan. 12, 2017), http://www.pewinternet.org/fact-sheet/internet-broadband/.

[3] U.S. Department of Commerce Internet Policy Taskforce & Digital Economy Leadership Team, *Fostering the Advancement of the Internet of Things*, 4 (Jan. 2017), *available at* https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

Organisation for Economic Cooperation and Development ("OECD") reports that in OECD countries, including the United States, a family of four today has ten devices connected to the Internet in their household, with that number expected to grow to 50 devices by 2022.[4] Smart devices have proliferated inside Americans' homes, cars, and even their bodies.[5]

Virtually all these connected devices and their associated applications transmit information through third-party providers. All modern communication tools—including e-mail, text, cloud-based photo storage, Voice over Internet Protocol, iMessage, Twitter, Google chat, Instagram message, and many others—depend on cable, ISP, Bluetooth, phone, and Wi-Fi services run by third parties. *See* Matthew Tokson, *Automation and the Fourth Amendment*, 96 Iowa L. Rev. 581, 602–04 (2011). Smartphones, smart homes, smart cars, and smart medical devices connected through the Internet of Things are only "smart" because of third-party interconnectivity. Andrew Guthrie Ferguson, *The Smart Fourth Amendment*, 102 Cornell L. Rev. 547, 557–59

---

[4] OECD Digital Economy Outlook, 255 (Paris: OECD Publishing, 2015), http://dx.doi.org/10.1787/9789264232440-en.

[5] Government Accountability Office, Center for Science, Technology and Engineering, *Technology Assessment: Internet of Things, Status and Implication of an Increasingly Connected World*, GAO-17-75, at 16–18 (May 2017); *see also* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 Tex. L. Rev. 85, 103–04 (2014) (discussing implantable health devices).

(2017). Millions of people share political and cultural opinions, news, and beliefs on third-party social media platforms. *See Packingham v. North Carolina*, 137 S. Ct. 1730, 1735 (2017). Internet searches and artificially intelligent assistants answer the most intimate and arcane questions through third-party search engines. *See United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (acknowledging the revealing nature of internet searches). Personal photographs, calendars, shopping lists, medical prescriptions, and an expanding network of contacts are housed in third-party storage. *See Riley v. California*, 134 S. Ct. 2473, 2491 (2014). Third-party data can be found in credit reports, employment histories, address changes, and retail purchases. Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. Pa. L. Rev. 327, 354–59 (2015). Families share their lives virtually, companies store their records electronically, and industries offer third-party technologies to service these expanding data-driven needs.

The ubiquity of third-party services has qualitatively changed our relationship with technology and each other. Indeed, one cannot effectively participate in the modern world without using these tools. To connect with friends, apply for jobs, receive medical services, or save photos from a family vacation, one must constantly transmit personal, "trackable" data to third-party services. Oftentimes these services collect location and other information through automation and without the user's knowledge or voluntary consent.

Third-party collection of intimate, personal data will only grow in the future. Companies have become adept at monetizing personal data, providing an ever-increasing incentive for them to collect more of it. Advances in connected technology will greatly expand the information that can be gleaned from data collected by third-party providers, going far beyond what is currently possible with CSLI data.[6] This will include the "content" of what is sent and saved, not merely the more neutral-seeming locational information that is at issue in this appeal.

The continuous data collection by smart devices and networks—from smart heating systems to smart heart stents—provides "a revealing montage of the user's life." *Riley*, 134 S. Ct. at 2490. For example, researchers have found that by simply studying vast sets of phone records they can predict who is in a relationship, sick, or involved in illicit activities.[7] Extending what some have called the third-party doctrine to digital third-party services could exempt all of this information from Fourth Amendment protection, potentially eliminating individual privacy in the modern age. *See* Margot E. Kaminski, *Robots in the Home: What Will We Have Agreed To?*, 51 Idaho L. Rev. 661, 670 (2015).

---

[6] *See* Brian Clark, *The Company Behind Roomba Cleaner Wants to Sell Home Data to Apple, Amazon, or Google*, Business Insider (July 25, 2017).

[7] Jonathan Mayer, Patrick Mutchler, & John C. Mitchell, *Evaluating the Privacy Properties of Telephone Metadata*, 113 PNAS 5536, 5540 (May 17, 2016).

B. Smith *Addressed a Radically Different Context Than This Case and Should Be Limited to Its Facts*

Smith was grounded in the particular context of dialed telephone numbers and mid-Twentieth-Century telephone routing. In *Smith*, the Court reasoned that Smith had no subjective expectation of privacy in the numbers he dialed because he very likely knew that the telephone company recorded the numbers of his long-distance phone calls. *Smith*, 442 U.S. at 742. His monthly bills revealed that the telephone company recorded his dialed phone numbers. *Id.* The telephone company also offered to check for overbilling and to identify callers making "annoying or obscene calls." *Id.* at 742–43. In short, because Smith affirmatively acted by dialing the phone numbers and had been informed repeatedly that the information was collected, he voluntarily conveyed the information to the third party, which in turn could choose to turn those numbers over to the government. *Id.* at 743–44. Nothing about the content of the communications was shared, only the identity of the individuals or businesses with whom a person communicated. *See id.*

When *Smith* was decided, society's relationship to technologies that transmitted information to third parties was very different than it is today.[8] The use

---

[8] Lower courts and states have struggled with the third-party doctrine in light of the increasing interconnectedness of modern society, with numerous jurisdictions rejecting its relevance to the modern era or limiting it to the facts of existing pre-digital-era cases. *See, e.g.*, *Commonwealth v. Estabrook*, 472 Mass. 852 (2015) (holding that a warrant was required to collect two weeks

of such tools was limited, and the transmission of information to third parties was clearly disclosed to users. *But see Smith*, 442 U.S. at 750 (Marshall J., dissenting) ("[U]nless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. . . . It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative."). More foundationally, the privacy implications of long-term, aggregated locational tracking from digital devices dwarf the privacy considerations in *Smith*. And extending *Smith*'s reasoning to define privacy today would have consequences beyond the criminal justice context, creating a chilling surveillance threat. Indeed, the differences between this case and *Smith* overwhelm any similarities.

First, as with all old-fashioned telephones, the user in *Smith* had to actively transmit numerical information to use the device (and thus reveal personal information). By contrast, cell phones can be tracked without the user making a call or sending a text. Cell phones periodically (roughly every 7 seconds) transmit a "registration" signal containing the phone's unique serial number. *See, e.g.*, James Beck et al., *The Use of Global Positioning (GPS) and Cell Tower Evidence to Establish a Person's Location—Part II*, 49 Crim. Law. Bull. 8 (Summer

---

of CSLI); *State v. Earls*, 70 A.3d 630 (N.J. 2013) (holding that a warrant was required to obtain cell phone tracking information); *see also* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 Cath. U. L. Rev. 373 (2006).

2013).[9] Simply by possessing a cell phone, an owner is revealing his or her location. This requires no affirmative act. Thus, CSLI cannot be analogized to *Smith*'s reasoning, which equated affirmative use (dialing a number) with a relinquishment of an expectation of privacy.

Second, *Smith* turned in large part on the Court's conclusion that the transmittal of information to a third party was "voluntary." *Smith*, 442 U.S. at 432–33; *but see id.* at 750 (Marshall J., dissenting). Today, cell phone users do not knowingly and voluntarily convey their location information to their cell phone companies. As a technological matter, the tracking is automatic and takes place between a phone and cell site without any volitional choice on the user's part. Indeed, recent empirical studies show that the majority of cell phone users do not even know that cell phone companies may be tracking and storing users' physical location via CSLI. One study found that only 26.5 percent of all cell phone users

---

[9] Registration data is routinely used by law enforcement. *See, e.g., In re Application of the U.S. for Historical Cell Site Data*, 2010 WL 4286365, at *1 (S.D. Tex. Oct. 29, 2010) ("[T]he Government seeks continuous location data to track the target phone over a two month period, whether the phone was in active use or not."); *United States v. Benford*, 2010 WL 1266507, at *1 (N.D. Ind. Mar. 26, 2010) (government sought information "identifying which cell tower communicated with the cell phone while it was turned on"); *In re Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & a Caller Identification Sys. on Tel. Numbers*, 402 F. Supp. 2d 597, 598 (D. Md. 2005) (government sought CSLI data identifying "the physical location of the person in possession of the cell phone whenever the phone was on."); *see also* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 Md. L. Rev. 681, 705–08 (2011).

understand that their cell phone provider is tracking and storing information on their physical location. Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 Nw. U. L. Rev. 139, 175–79 (2016). Even fewer cell phone users are actually aware of cell-signal-based location tracking. When the minority of users who thought that tracking occurs was asked as a follow-up question to describe how their cell service provider collects information on their location, only 12.7 percent of these users gave a response that could be interpreted as referring to cell-site or cell-signal tracking. *Id.* at 177. Altogether, only 3.3 percent of all cell phone users surveyed gave responses that indicated awareness of CSLI tracking. *Id.* Cell phone users simply do not voluntarily convey any location information to their cell service providers and do not know that they are inadvertently conveying such information. This shared but mistaken belief by the general public that the possession of a cellphone does not submit someone to constant, recorded location tracking reflects the expectation of privacy that people have about their location information.

Third, location tracking is far more invasive than obtaining a monthly record of dialed numbers. CSLI tracking can reveal everywhere that a person goes for as long as he or she owns a cell phone—which, for most of us, will be the remainder of our adult lives. This data can track a person's movements with precision, and will become only more precise as technology improves, more cellular devices are used, and more cell towers are built.[10]

---

[10] When petitioner Timothy Carpenter's records were obtained in 2011, CSLI was already able to pinpoint a person's location

Information that reveals a person's location can reveal "trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the hy-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on." *People v. Weaver*, 12 N.Y.3d 433, 441–42 (2009). This information becomes even more revealing when aggregated and collected over long periods of time. *See United States v. Maynard*, 615 F. 3d 544, 562 (D.C. Cir. 2010) (*aff'd on other grounds sub nom Jones*, 565 U.S. 400). Service providers retain location data for long periods of time: AT&T for five years, Sprint for 18 months, and Verizon for one year. Pet. Br. at 20.

Location data therefore yields "a highly detailed profile, not simply of where we go, but by easy inference, of our associations—political, religious, amicable and amorous, to name only a

---

within a .1 square mile area. Stephen E. Henderson, *Carpenter v. United States and the Fourth Amendment: The Best Way Forward*, 26 William & Mary Bill of Rights J. (forthcoming 2017), *available at* https://works.bepress.com/stephen_henderson/55/. Over the past decade, the number of cell sites has increased from 195,613 to 308,334, a trend that will only continue as an ever-increasing number of consumers demand ever-faster and more reliable cell service. *See* CTIA. *Annual Year-End 2016 Top-Line Survey Results*, https://www.ctia.org/docs/default-source/default-document-library/annual-year-end-2016-top-line-survey-results-final.pdf?sfvrsn=2 CSLI; *cf. Kyllo v. United States*, 533 U.S. 27, 36 (2001) ("While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.").

few—and of the pattern of our professional and avocational pursuits." *Weaver*, 12 N.Y. 3d at 442. Such data gives much more information about a person and his or her activities than does a list of phone numbers dialed. It is a modern-day panopticon of constant surveillance enabled by the necessary use of a cellphone.

Lastly, the data at issue here is distinguishable from that revealed in *Smith* because it has expressive value, and allowing law enforcement unfettered access to such information has far-reaching consequences beyond impacting privacy. An unchecked third-party doctrine creates a chilling surveillance threat that threatens associational liberty, free expression, and intellectual growth, undermining the democratic health of the nation. *See* Neil M. Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934, 1936, 1940 (2013). Law enforcement's constitutionally unfettered access to every third-party data point means any citizen questioning the government—be they a journalist, judge, protestor, or pariah—will be at risk of being exposed through aggregated and collected personal third-party data. There is evidence that arbitrary, invasive, or overbroad requests of third-party providers have already proliferated, and will continue to do so without a constitutional check. *See* Spenser Hsu, *Court: Warrantless Requests to Track Cellphones, Internet Use Grew Sevenfold in D.C. in Three Years*, Wash. Post (July 18, 2017). The awareness that the government may at some point—even five years from now—review data revealing one's every movement will have chilling effects on controversial or even merely embarrassing conduct,

diminishing the ability of individuals to exercise their rights and freedoms. *See* Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. Rich. L. Rev 465, 474 (2015) (discussing studies that show changes in online user habits in response to public disclosure of government surveillance); Alex Matthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior* (April 29, 2015), https://www.ftc.gov/system/files/documents/public_comments/2015/10/00023-97629.pdf (showing that Google searches for controversial topics decreased following the public revelation of the NSA's internet surveillance programs).

These crucial differences between *Smith* and this case apply to all smart devices. Most devices are designed to work automatically without user action, affirmatively thwarting the user's ability to make voluntary choices about information they choose to convey to third parties. These distinctions -and the threats to privacy and liberty posed by warrantless collection of data from third parties—will only be exacerbated as digital technology develops.

II. THE THIRD-PARTY DOCTRINE HAS BEEN WIDELY CRITICIZED BY SCHOLARS

For these reasons and others, almost every scholar to have written on the subject has called for the demise of the third-party doctrine enunciated in *Smith* as applied in the digital context. Many scholars have noted that the doctrine is based on a questionable theory of privacy, as most people do not

think of information disclosed to others for a limited purpose as no longer private for other purposes. *See, e.g.*, Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 Vand. L. Rev. 1289, 1315 (1981); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. Law Rev. 1083, 1135 (2002). Others have focused on the doctrine's inaptness to the expectations of privacy in the digital age. *See, e.g.*, Tokson, *Knowledge and Fourth Amendment Privacy*, 111 Nw. U. L. Rev. at 175–79; Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 Sup. Ct. Rev. 205 (2015); Christopher Slobogin, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 184–86 (2007). Although the doctrine has a vocal defender, *see* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561 (2009),[11] the justifications offered do not hold up in the digital age. This Court should decline to extend the doctrine now, in line with the overwhelming weight of scholarly literature on the topic.

---

[11] Even Orin Kerr, the doctrine's chief defender, admits that "[i]t is the *Lochner* of search and seizure law, widely criticized as profoundly misguided." Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. at 563. Indeed, he notes, "[t]he verdict among commentators has been frequent and apparently unanimous: The third-party doctrine is not only wrong, but horribly wrong." *Id.*

A. The Third-Party Doctrine Is Based on a Questionable Theory of Privacy

The third-party doctrine's central tenet is that once an individual discloses information to any third party for any purpose, no matter how confidential, that citizen irrevocably sets aside any reasonable expectation that the government will not obtain that information from the third party without a warrant issued upon probable cause. This does not, however, accord with the expectations most people have when transmitting information for a specific purpose. As such, even setting aside the serious issues presented by the digital age, many scholars believe the third-party doctrine is based on a highly questionable premise.

Most people recognize that "[p]rivacy is not an all or nothing phenomenon." Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 Vand. L. Rev. at 1315; *Smith*, 442 U.S. at 749 (Marshall J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."). In disclosing information to a business, health care provider, or other third party, an individual has a reasonable expectation that his information will be used for a limited purpose and will not be disclosed to any other party without their permission. *See, e.g.*, Wayne R. La Fave, 1 SEARCH AND SEIZURE, A TREATISE ON THE FOURTH AMENDMENT § 2.7(c) (5th ed. 2012); *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001)

(concluding that hospital patients had a reasonable expectation of privacy in test results because the results were not disclosed to any other party without the patients' permission); *see also* Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 Fordham L. Rev. 611, 612 (2014) (arguing that when information is shared for the sole purpose of obtaining an indispensable social good, the third party's cooperation with law enforcement should be analyzed as a Fourth Amendment search). In particular, it is unreasonable to consider data somehow "not private" if the information, like CSLI, is generally exposed only to automated systems rather than human employees. *See* Tokson, *Automation and the Fourth Amendment*, 96 Iowa L. Rev. at 611–27.

Moreover, the idea that the third-party doctrine applies even in cases where—like here—the government coerces a third party into disclosing such information is highly problematic. The doctrine was originally premised on the idea that individuals "assumed the risk" that an associate would choose to talk to the police. *See Hoffa v. United States*, 385 U.S. 293, 302 (1966). Allowing the police to coerce third parties into disclosing confidential information threatens to eliminate privacy in countless forms of personal information, and contradicts the reasoning of *Katz*—as surely it would have been a Fourth Amendment "search" if, in *Katz*, the government ordered the phone company to tap its own wires, even

though the company has the legal right to record phone conversations in several situations.[12]

As such, scholars and commentators overwhelmingly consider the third-party doctrine a perversion of the *Katz* test that fails to accurately consider either social norms or actual expectations of privacy. *See, e.g.*, Stephen Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 Iowa L. Rev. Bull. 39 (2011); Jed Rubenfeld, *The End of Privacy*, 61 Stan. L. Rev. 101, 113–14 (2008); Jack M. Balkin, *Essay: The Constitution in the National Surveillance State*, 93 Minn. L. Rev. 1, 19 (2008); Slobogin, PRIVACY AT RISK at 151–64; Susan Freiwald, *First Principles of Communications Privacy*, 2007 Stan. Tech. L. Rev. 3, 46–49 (2007); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & Pol'y 211, 242–44 (2006); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557, 1571 (2004); Sherry Colb, *What Is a Search: Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 Stan. L. Rev. 119 (2002); Daniel J. Solove, *Digital Dossiers*

---

[12] *See* 18 U.S.C. § 2511(2)(a)(i) ("It shall not be unlawful under this chapter for . . . an officer, employee, or agent of a provider of wire or electronic communication service . . . to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service."); *id.* § 2511(2)(a)(ii) (providing for telephone company compliance with law-enforcement requests).

and the Dissipation of Fourth Amendment Privacy, 75 S. Cal. Rev. 1083, 1093–94 (2002); Scott E. Sundby, *Everyman's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 Colum. L. Rev. 1751, 1757–58 (1994); James Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward An Expanded Vision of the Fourth Amendment Privacy Province*, 36 Hastings L. J. 645 (1985); Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 Mich. L. Rev. 1229, 1254–56 (1983).

B. The Third-Party Doctrine Does Not Match Expectations of Privacy in the Digital Age

Scholars have noted that the underlying assumptions behind the third-party doctrine concerning expectations of privacy and the consensual disclosure of information become even more misplaced in the digital age. Citizens have come to depend on third parties for vital services, and they lack adequate alternatives for these services. When engaging in everyday modern life, people do not expect that exposing personal information to one party means forgoing a reasonable expectation of privacy toward all others, including the police. As discussed above, few people are even aware that they are disclosing such information and on a vast and constant scale. Moreover, scholars have recognized that the artificial distinctions created as a compromise to avoid the privacy-destroying consequences of the third-party doctrine no longer work in the age of data. Chris Conley, *Non-Content Is Not Non-Sensitive: Moving Beyond the Content/non-Content Distinction*, 54 Santa Clara L.

Rev. 821, 831 (2014); Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends* Katz, Smith, *and Electronic Surveillance Law*, 30 Harv. J.L. & Tech. 1 (2016).

In particular, distinctions between public/private activities and content/non-content information fail to justify the third-party doctrine when applied to information sharing and long-term, aggregated, public surveillance. Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 Cardozo L. Rev. 643, 658 (2013); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 Pepp. L. Rev. 975, 1020–24 (2007). In certain circumstances, an aggregation of supposedly "non-content" location information can be as revealing as "content," just as public actions can reveal private expressive acts. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring). A full embrace of the third-party doctrine in the digital era would imply that individuals have no reasonable expectation of privacy in e-mails stored on third-party servers, electronic health records, and all third-party information linked to our smartphones. Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 Md. L. Rev. 614, 642 (2011); *see also United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (holding that the Fourth Amendment protects e-mail content).

Even isolated defenders of the third-party doctrine concede that justifying it on reasonable expectation of privacy grounds is "awkward and unconvincing," and assert that it is better conceptualized as a consent doctrine. Kerr, *The Case*

for the Third-Party Doctrine, 107 Mich. L. Rev. at 588. But this fallback argument of consent has itself been challenged as theoretically inadequate and practically inaccurate. Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 Berkeley Tech. L.J. 1199, 1206 (2009). And as a technological matter, in the context of CSLI and smart devices, the automated nature of ubiquitous and involuntary connection undercuts the consensual nature of the exposure.

The reality is this: There is no principled way to limit *Smith* once applied in the digital context. If *Smith* applies here, the proponents of warrantless CSLI cannot foreclose the extension of the third-party doctrine to authorize the disclosure of the content of our cyber-lives. The Court need not proceed down this path.

C. Justifications for the Third-Party Doctrine Do Not Hold Up in the Digital Age

The primary defender of the doctrine claims the rule is required for two reasons: first, to preserve a privacy/security balance built into the reasonable expectation of privacy test; and second, to develop clear *ex ante* rules for police to follow. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. at 584–85. Both justifications fall apart when applied to the invasive, precise, automatic, and involuntary data revealed to third parties in the digital age.

First, the technological landscape of the *Smith* era has been replaced by a world in which there exists an abundance of third-party data available to

law enforcement. The digital footprints we leave are extensive and exposing. If there is a need to rebalance the risks of privacy and security, the balance should shift toward limiting unfettered access to location data and other personal information. *See, e.g.*, Slobogin, PRIVACY AT RISK at 6–9; Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, 2011 U. Ill. J.L. Tech. & Pol'y 281, 285 (2011). In a world of big data policing, the ability to rummage among the available digital clues empowers law enforcement at the expense of citizens. Andrew Guthrie Ferguson, THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT 17–18, 129 (2017).

The second justification for the third-party doctrine turns on a stated need for *ex ante* clarity for law enforcement. Trying to divine exactly which information is protected in third-party business records is just too difficult, the argument goes. The third-party doctrine's simplistic answer is to assert that the individual loses all Fourth Amendment interest in the data shared with another party.

While clear, this solution is wrong and unnecessary. The better answer is that both the individual and the third party retain Fourth Amendment rights in the information produced and possessed by the individual, and the information produced and possessed by third parties. In a variety of circumstances—a renter living in a rented house, a package handed to a common courier, an e-mail on a third-party server—the Fourth Amendment recognizes that both owner and user have overlapping Fourth Amendment privacy rights. *See, e.g.*, *Georgia v. Randolph*, 547 U.S. 103, 114 (2006);

Chapman v. United States, 365 U.S. 610, 616-18 (1961); *Stoner v. California*, 376 U.S. 483, 489 (1964); *United States v. Jeffers*, 342 U.S. 48, 52 (1951); *see also* Tokson, *Automation and the Fourth Amendment*, 96 Iowa L. Rev. at 630–31. The same should be true for digital information serviced by third parties. Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & Pol'y 211, 245–65 (2006); Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 Calif. L. Rev. 1593, 1593–1600 (1987). In fact, this duality is even more relevant in the digital age as the same information might be possessed simultaneously by the user and the third party. As the Court recognized in *Riley*, for example, information on a smart device may be stored locally and also on the cloud. *Riley*, 134 S. Ct. at 2491.

Allowing both user and third party to possess Fourth Amendment rights in this data would not create a logistical challenge for law enforcement. Even in the absence of the third-party doctrine, third-party service providers faced with government requests for user data would not need to calculate their users' Fourth Amendment rights. Just as in any other Fourth Amendment context, it is the government's responsibility to secure a warrant for an individual's personal data, whether stored by third-party services or otherwise.

So, for example, if the government wants to access collected data from a "smart" pacemaker to

investigate a crime,[13] the question is not who owns the digital content or who possesses the personal data, but what justification the police have for requesting the information.[14] Just like the other situations involving rental property, hotels, and couriers with overlapping privacy interests, law enforcement cannot merely ignore the privacy interests of one party by focusing on the other's ownership. Instead, because of the overlapping Fourth Amendment interests, police must get a warrant. This requirement offers equally clear *ex ante* "guidance to law enforcement through categorical rules." *See Riley*, 134 S. Ct. at 2491. While not simplistic, applying the traditional

---

[13] *See* Cleve R. Wootson, Jr., *A Man Detailed His Escape from a Burning House. His Pacemaker Told Police a Different Story*, Wash. Post (Feb. 8, 2017).

[14] Further, framing the argument about access to existing business records is a bit misleading. Be it CSLI or smart health data, these sought after digital "records" do not exist in some electronic filing cabinet of "records." The vast amount of digital information pinging from every cell tower and smart home is only seen by automated, computer collection systems and largely undifferentiated to the third-party collector. Tokson, *Automation and the Fourth Amendment*, 96 Iowa L. Rev. at 604. To obtain specific information about a specific customer in response to a law enforcement request, the companies must affirmatively search the relevant datasets. If those datasets contain personal information (like the aggregated locational information of an individual) then the exposing, personal nature of the process becomes obvious. It is only by organizing the otherwise unanalyzed data that the relevant datasets get created. It is, thus, inaccurate to frame the issue as merely a request for business records from already created business data. The records—including personalized data—are created in response to a law enforcement request, and thus expose personal information in response to a law enforcement request.

reasonable expectation of privacy test and warrant requirement has been shown to work well enough and can be adapted to the digital age of locational tracking and smart devices.

Revealingly, a warrant requirement has been the default policy for major technology companies when it comes to requests for digital content held by third parties. Amazon, Apple, Dropbox, Facebook, Google, Lyft, Microsoft, Pinterest, Twitter, WordPress, and Yahoo among other third parties all require a lawful warrant to obtain the content of user data. *See* Nate Cardozo et al., *Who Has Your Back?: Protecting Your Data from Government Requests*, Elec. Frontier Found. 6–8, 12 (July 2017). To be precise, the company policies protect "content," nominally tracking the artificial content/non-content distinction between protected and unprotected communications being held by third parties. *See* Orin S. Kerr, *Applying the Fourth Amendment to Internet Communications: A General Approach*, 62 Stan. L. Rev. 1005, 1019–20 (2010). But, in practice, some companies' definition of "content" embraces location information and even shared public content. For example, the transportation company Lyft requires a warrant for "prospective cell tracking" (real-time tracking),[15] and Uber requires a warrant for GPS location information.[16] Third-party services like

---

[15] *Law Enforcement Requests*, Lyft, https://help.lyft.com/hc/en-us/articles/214218437-Law-Enforcement-Requests ("We will require a warrant for requests for content of communications between Users or for prospective location data.").

[16] *Uber Guidelines for Law Enforcement Authorities*, Uber, https://www.uber.com/legal/data-requests/guidelines-for-law-enforcement-united-states/en-US/ ("We require . . . [a] search

Facebook (which exists to share ideas, photos, and communications with others) still requires law enforcement to obtain a warrant before providing those shared ideas, photos, and location information to law enforcement.[17] The practice shows that consumers expect third parties to protect their personal information and that a warrant requirement for such information can be workable for companies and law enforcement.[18] This final point—that law enforcement manages to secure necessary data

---

warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel our disclosure of certain communications between people using Uber or GPS location information.").

[17] *Information for Law Enforcement Authorities*, Facebook, https://www.facebook.com/safety/groups/law/guidelines/, ("A search warrant issued under the procedures described in the Federal Rules of Criminal Procedure or equivalent state warrant procedures upon a showing of probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, timeline posts, and location information.").

[18] Facebook reported that the company received 14,736 warrant requests between July and December 2016, and that it provided some information 85.32 percent of the time. *Government Requests Report*, Facebook, https://govtrequests.facebook.com/country/United%20States/2016-H2/. Uber reported that the company received 205 warrant requests during the same time period, and that it provided some data 87 percent of the time. *Transparency Report*, Uber, https://transparencyreport.uber.com/. In 2015, the company received 16 search warrants, fully complied with 12, partially complied with three, and did not respond to one. *Lyft Information Request Report – 2015*, Lyft, https://lyft-assets.s3.amazonaws.com/helpcenter/Drive%20With%20Lyft/Lyft%20Transparency%20Report%20-%202015%20(1).pdf.

through warrants—demonstrates that a better balance between privacy and security can be struck.

CONCLUSION

The so-called third-party doctrine has been widely criticized by scholars for decades, and its underpinnings continue to erode. Both as a matter of privacy theory and due to practical concerns regarding today's technologies, the foundations no longer hold. Mechanical application of *Smith v. Maryland* to a digital age will undermine privacy and amplify mass surveillance in ways that threaten associational freedom and personal liberty. New technologies and new expectations of privacy require a new approach. To ensure that the Fourth Amendment protects privacy in the future as it has in the past, this Court should limit *Smith* to its unique facts, or otherwise reject the third-party doctrine outright.

Dated: August 14, 2017

Respectfully submitted,

ANDREW G. FERGUSON
UDC David A. Clarke School of Law
4340 Connecticut Ave.
Washington, D.C. 20008

HARRY SANDICK
Counsel of Record
KATHRINA SZYMBORSKI
JARED BUSZIN
Patterson Belknap Webb & Tyler LLP
1133 Avenue of the Americas
New York, NY 10036
(212) 336-2000
hsandick@pbwt.com

Counsel for *Amici Curiae*

APPENDIX A[19]

Barbara Babcock
Founder and former Director of the Public Defender Service in Washington, D.C.
Crown Professor of Law, Emerita
Stanford Law School

Jordan M. Blanke
Ernest L. Baskin, Jr. Distinguished Professor of Computer Information Systems and Law
Stetson School of Business & Economics
Mercer University

Robert M. Bloom
Professor of Law
Boston College Law School

Kiel Brennan-Marquez
Research Fellow, New York University School of Law
Visiting Fellow, Information Society Project, Yale Law School

Edwin J. Butterfoss
Professor of Law
Mitchell Hamline School of Law

Robert Calhoun
Professor of Law Emeritus
Golden Gate Law School

Adam Candeub

---

[19] *Amici curiae* appear in their individual capacities; institutional affiliations are provided here for identification purposes only.

Professor of Law
Director, IP, Information, & Communications Law Program
Michigan State University

Bennett Capers
Stanley A. August Professor of Law
Brooklyn Law School
Visiting Professor at Boston University School of Law (Fall 2017)

Jenny Carroll
Professor of Law
University of Alabama

Gabriel J. Chin
Edward L. Barrett Jr. Chair and Martin Luther King Jr. Professor of Law
UC Davis School of Law

Ralph D. Clifford
Professor of Law
University of Massachusetts Law School

Joshua Fairfield
William Donald Bain Family Professor of Law
Washington and Lee University

Andrew Guthrie Ferguson
Professor of Law
UDC David A. Clarke School of Law

James Grimmelmann
Professor of Law
Cornell Tech and Cornell Law School

Susan Freiwald
Associate Dean of Academic Affairs and Professor of Law
USF School of Law

Woodrow Hartzog
Professor of Law and Computer Science
Northeastern University
School of Law
College of Computer and Information Science

Janet C. Hoeffel
Catherine D. Pierson Professor of Law
Tulane University School of Law

David Jaros
Associate Professor of Law
University of Baltimore School of Law

Margot E. Kaminski
Associate Professor of Law
Colorado Law

Mark A. Lemley
William H. Neukom Professor
Stanford Law School

Dave Levine
Associate Professor
Elon University School of Law
Affiliate Scholar, Stanford Law School Center for Internet and Society

Richard H. McAdams
Bernard D. Meltzer Professor of Law
University of Chicago Law School

Thomas M. McDonnell
Professor of Law
Elisabeth Haub School of Law at Pace University

William McGeveran
Professor of Law and Solly Robins Distinguished Research Fellow
University of Minnesota Law School

Colin Miller
Professor and Associate Dean for Faculty Development
University of South Carolina School of Law

Steven J. Mulroy
Professor of Law
Humphreys School of Law, University of Memphis

Connie Davis Nichols
Professor of Law
Baylor Law School

Kenneth B. Nunn
Professor of Law
University of Florida, Levin College of Law

Paul Ohm
Professor of Law
Georgetown University Law Center

Brian L. Owsley
Assistant Professor of Law
UNT Dallas College of Law

Blake Reid
Associate Clinical Professor
Colorado Law

Neil Richards
Thomas & Karole Green Professor of Law
Washington University in St. Louis

David Rudovsky
Senior Fellow
Penn Law School

Jason Schultz
Professor of Clinical Law
New York University School of Law

Victoria L Schwartz
Associate Professor of Law
Pepperdine University School of Law

Dawinder S. Sidhu
Of Counsel, Shook, Hardy & Bacon, LLP
Visiting Professor, University of Baltimore School of Law

Priscilla J. Smith
Clinical Lecturer in Law
Director and Senior Fellow, Program for the Study of Reproductive Justice
Yale Law School

Randolph N. Stone
Clinical Professor of Law
University of Chicago Law School

Kim Taylor-Thompson
Professor of Clinical Law
New York University School of Law

George C. Thomas III
Rutgers University Board of Governors Professor of Law
Judge Alexander P. Waugh, Sr. Distinguished Scholar

Ari Ezra Waldman
Associate Professor of Law
New York Law School

Jonathan Weinberg
Professor of Law
Wayne State University